Application Serial No. 10/813,369
Client/Matter No. 6270/139

In the Claims:

The status of the claims is as follows. This listing of claims replaces all prior versions and listings of claims in the application.

1. (Original) An energy management device for use in an energy management architecture for managing an energy distribution system, said energy management architecture including a network, said energy management device comprising:

an energy distribution system interface operative to couple said energy management device with at least a portion of said energy distribution system;

a network interface operative to couple said energy management device with said network for transmitting outbound communications to said network, said outbound communications comprising energy management data;

a processor coupled with said network interface and said energy distribution system interface, operative to generate said energy management data;

a tamper prevention seal coupled with said energy management device, operative to substantially deter unauthorized access to said energy management device and indicate any such access; and

a seal tamper detection unit coupled with said processor and said tamper prevention seal and operative to detect when said tamper prevention seal indicates that unauthorized access has occurred.

2. (Original) The energy management device of Claim 1, wherein said tamper seal comprises a revenue seal.

3. (Original) The energy management device of Claim 1, wherein said tamper seal comprises a metering point id seal.

4. (Original) The energy management device of Claim 1, further comprising a memory coupled with said processor, said memory operative to store confidential data.

5. (Original) The energy management device of Claim 4, wherein said processor is further operative to delete said confidential data from said memory when said seal tamper

detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred.

6. (Original) The energy management device of Claim 4, wherein said processor is further operative to prevent access to said confidential data when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred.

7. (Original) The energy management device of Claim 4, wherein said confidential data comprises a private key operative to sign said energy management data.

8. (Original) The energy management device of Claim 7, wherein said processor is further operative to delete said private key from said memory when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred.

9. (Original) The energy management device of Claim 7, wherein said processor is further operative to send a message warning that said tamper prevention seal has been tampered with through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred, and to sign said message with said private key.

10. (Original) The energy management device of Claim 4, wherein said confidential data comprises a certificate operative to sign said energy management data.

11. (Original) The energy management device of Claim 10, wherein said processor is further operative to delete said certificate from said memory when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred.

12. (Original) The energy management device of Claim 1, wherein said processor is further operative to prevent said transmitting of said energy management data through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred.

13. (Original) The energy management device of Claim 1, wherein said processor is further operative to prevent said transmitting of signed energy management data through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred.

14. (Original) The energy management device of Claim 1, wherein said processor is further operative to send a message warning that said tamper prevention seal has been tampered with through said network interface when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred.

15. (Original) The energy management device of Claim 1, further comprising a memory coupled with said processor and operative to store at least one device setting and wherein said processor is further operative to prevent changes to said at least one device setting when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred.

16. (Original) The energy management device of Claim 1, further comprising a memory coupled with said processor and operative to store at least one device setting and wherein said processor is further operative to send a message warning that said device setting has been changed through said network interface when said at least one device setting has been changed after said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred.

17. (Original) The energy management device of Claim 1, further comprising a memory coupled with said processor and operative to store a device configuration, said device configuration having at least one first device setting having a first value, said processor being operative to generate said energy management data based on said first value and to determine that said at least one first device setting has been modified to at least one second value after said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred, said processor being further operative to generate said energy management data based on said first value and generate alternate energy management data based on said at least one second value in response to said modification.

18. (Original) The energy management device of Claim 1, wherein said processor is further operative to block external access to said energy management device when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred.

19. (Original) The energy management device of Claim 1, wherein said processor is further operative to create an audit log when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred.

20. (Currently Amended) The energy management device of Claim 19, wherein said processor is further operative to at least one of hashing and encrypting said audit log.

21. (Original) The energy management device of Claim 1, wherein said processor is further operative to set off a security alarm when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred.

22. (Original) The energy management device of Claim 1, further comprising a display coupled with said processor and operative to visually display text, and wherein said processor is further operative to place a warning message on said display when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred.

23. (Original) The energy management device of Claim 1, wherein said processor is further operative to mark said energy management data as unreliable when said seal tamper detection unit detects that said tamper prevention seal indicates that unauthorized access has occurred.

24. (Original) The energy management device of Claim 1, wherein said seal tamper detection unit further comprises a sensor operative to detect that said tamper prevention seal is broken.

25. (Original) The energy management device of Claim 24, wherein said sensor comprises a limit switch.

26. (Original) The energy management device of Claim 24, wherein said sensor comprises a proximity sensor.

27. (Original) The energy management device of Claim 26, wherein said proximity sensor comprises at least one of a pin, an optical proximity sensor, an optical motion detector, a grounding tab, an ultrasonic sensor, an electro-magnetic sensor and a gyroscope.

28. (Original) The energy management device of Claim 24, wherein said sensor comprises at least one of a camera and a video camera.

29. (Original) The energy management device of Claim 1, further comprising an energy storage device coupled with said seal tamper detection unit and operative to provide power to said seal tamper detection unit in power outage situations.

30. (Currently Amended) The energy management device of Claim 1, wherein said processor is further operative to perform at least one energy management function on said at least a portion of said energy distribution system ~~network~~ via said energy distribution system interface, said processor further operative to generate said energy management data as a function of said energy management function.

31. (Original) The energy management device of Claim 1, further comprising:

an enclosure defining an interior and an exterior and operative to enclose said energy management device within said interior and to limit access to said energy management device, and further wherein said tamper prevention seal is coupled with said enclosure and operative to substantially deter unauthorized access to said interior of said enclosure and indicate any such access.

32. (Original) A method of protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal operative to substantially deter unauthorized access to said energy management device and indicate any such access, the method comprising:

a) generating said data, said data being characterized by an integrity;

b) detecting when said tamper prevention seal indicates that unauthorized access has occurred; and

c) protecting said integrity of said data in response to said detecting.

33. (Original) The method of Claim 32, further wherein said energy management device stores confidential data, and wherein c) further comprises deleting said confidential data.

34. (Original) The method of Claim 32, further wherein said energy management device stores confidential data, and wherein c) further comprises preventing access to said confidential data.

35. (Original) The method of Claim 32, wherein c) further comprises preventing transmission of said data.

36. (Original) The method of Claim 32, wherein c) further comprises preventing signing of said data.

37. (Original) The method of Claim 32, wherein c) further comprises generating a warning message.

38. (Original) The method of Claim 32, further wherein said energy management device stores device settings, and wherein c) further comprises preventing changes to said device settings.

39. (Original) The method of Claim 32, further wherein said energy management device stores device settings, and wherein c) further comprises generating a warning message if said device settings are changed.

40. (Original) The method of Claim 32, further wherein said energy management device stores at least one first device configuration, said device configuration having at least one first device setting having a first value, said generating comprising generating said data based on said first value, the method further comprising d) detecting that said at least one first device setting has been modified to have at least one second value, and wherein c)

further comprises generating alternate data based on said at least one second value in addition to said data.

41. (Original) A system for protecting data created, stored and sent by an energy management device that is protected by a tamper prevention seal operative to substantially deter unauthorized access to said energy management device and indicate any such access, comprising:

means for generating said data, said data characterized by an integrity;

means for detecting when said tamper prevention seal indicates that unauthorized access has occurred; and

means for taking action to protect said integrity of said data.